# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 05-181418
(43)Date of publication of application : 23.07.1993

(51)Int.Cl. G09C 1/00
H04L 9/06
H04L 9/14

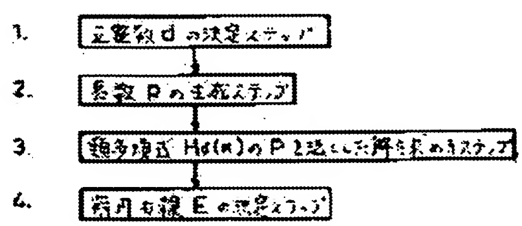
(21)Application number : 04-168007
(22)Date of filing : 25.06.1992

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : MIYAJI MITSUKO
TATEBAYASHI MAKOTO

(30)Priority
Priority number : 03158205 Priority date : 28.06.1991 Priority country : JP

## (54) OPEN KEY CIPHERING COMMUNICATION SYSTEM USING ELLIPTIC CURVE

(57)Abstract:
PURPOSE: To provide many elliptic curves which are embedded in a finite body, can not be solved, and are on definition bodies having the same number of bits.
CONSTITUTION: The open key ciphering communication system is based upon the difficulty of the discrete logarithmic problem of the elliptic curve; and the elliptic curve which is necessary for the open key ciphering communication system for an optional prime number (p) is constituted while having the finite body GF (p) on the definition body and (p) elements on the finite body GF (p). Therefore, when the elliptic curve E1 on the finite body GF (p) is given, #E1 (GF(p))=p is satisfied, so prime factorization is not necessary.



LEGAL STATUS

[Date of request for examination] 12.07.1996

[Date of sending the examiner's decision of rejection] 12.01.1999

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

| | |
|---|---|
| [Date of registration] | |
| [Number of appeal against examiner's decision of rejection] | 11-02202 |
| [Date of requesting appeal against examiner's decision of rejection] | 12.02.1999 |
| [Date of extinction of right] | |

THIS PAGE BLANK (USPTO)

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平5－181418

(43)公開日　平成5年(1993) 7月23日

| (51)Int.Cl.^5 | | 識別記号 | 庁内整理番号 | F I | | 技術表示箇所 |
|---|---|---|---|---|---|---|
| G09C | 1/00 | | 9194－5L | | | |
| H04L | 9/06 | | | | | |
| | 9/14 | | | | | |
| | | | 7117－5K | H04L | 9/ 02 | Z |

審査請求　未請求　請求項の数3(全 18 頁)

(21)出願番号　特願平4－168007

(22)出願日　平成4年(1992) 6月25日

(31)優先権主張番号　特願平3－158205

(32)優先日　平3(1991) 6月28日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　宮地　充子
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　館林　誠
大阪府門真市大字門真1006番地　松下電器産業株式会社内

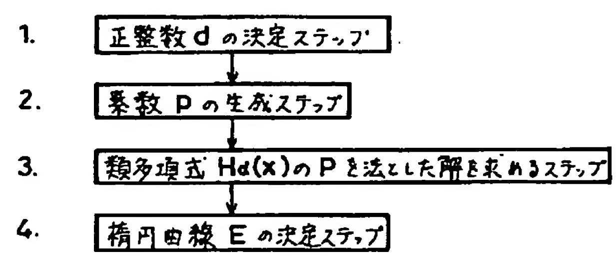
(74)代理人　弁理士　中島　司朗

(54)【発明の名称】　楕円曲線を用いた公開鍵暗号通信方式

(57)【要約】

【目的】　有限体に埋め込んで解くことが不可能、かつ同じビット数の定義体上の楕円曲線を豊富に提供可能とする。

【構成】　楕円曲線の離散対数問題の困難性に基礎をおく公開鍵暗号通信方式において、任意の素数ｐに対して公開鍵暗号通信方式に必要な楕円曲線を、有限体ＧＦ（ｐ）を定義体に持つ楕円曲線であって有限体ＧＦ（ｐ）上の元をｐ個持つように構成する。



【特許請求の範囲】

【請求項１】　数値化した通信文をＥ（ＧＦ（ｐ））の元と演算をなすことにより秘密通信若しくは署名通信を実現する公開鍵暗号通信方式において、
ｐを素数とし、有限体ＧＦ（ｐ）を定義体にもつ楕円曲線ＥのＧＦ（ｐ）上の元で構成される群をＥ（ＧＦ（ｐ））とするとき、
Ｅ（ＧＦ（ｐ））の元の個数がｐになるように楕円曲線Ｅをとり、
前記Ｅ（ＧＦ（ｐ））上定義される離散対数問題の困難さを公開鍵暗号通信方式の安全性の根拠にもつことを特徴とした楕円曲線を用いた公開鍵暗号通信方式。

【請求項２】　ＧＦ（ｐ）を定義体にもつ楕円曲線Ｅは、
正整数ｄを、虚二次体Ｑ（（－ｄ）$^{1/2}$）の類数が小さくなるようにとり、
素数ｐを、４＊ｐ－１＝ｄ＊平方数　の関係を充たすようにとり、
ｄにより定まる類多項式$H_d$（ｘ）＝０のｐを法とした解をｊ不変数にもつようにして得られることを特徴とする請求項１記載の楕円曲線を用いた公開鍵暗号通信方式。

【請求項３】　虚二次体Ｑ（（－ｄ）$^{1/2}$）の類数が１であることを特徴とする請求項２記載の楕円曲線を用いた公開鍵暗号通信方式。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は数値化された情報を公開通信網や放送網を使用して秘密送信する技術に関する。

【０００２】

【従来の技術】従来より、通信技術の一つである公開鍵暗号通信方式は、通信相手が多数の場合に、通信相手ごとに異なる暗号鍵を容易に管理可能しかも解読困難な方式であるため、公開された通信網を使用してのデータの秘匿や通信相手の認証及び署名などに際して、不特定多数の通信相手と通信を行うのに不可欠な基盤技術である。そして、この公開鍵暗号を用いて、たとえ盗聴等がなされたとしても、特定の通信相手以外に通信内容を漏らすことがない秘密通信方式が実現されている。更に、その応用としての特定の者のみが受信内容を解読し利用可能な放送や、専用の復号設備を有する者のみが利用可能な映画用レーザーディスクの貸し出しへの応用等も検討若しくは実用化されている。

【０００３】さて、この公開鍵暗号の安全性の根拠にはしばしば有限可換群上の離散対数問題（ＤＬＰ）の困難性が用いられる。有限可換群上の離散対数問題については、例えば、イ．バッハ　著　“イントラクタブル　プロブレムズ　イン　ナンバーシオリー”　アドバンス　インクリプトロギープロシーディングス　オブ　クリプト’８８．レクチャーノート　イン　コンピューターサイエンス，４０３（１９８８），シュプリンガー書店発行７７～９３頁（E. Bach. “Intractableproblems in number theory ”, Advances in Cryptology-Proceedings ofCrypto ’88. Lecture Notes in Computer Science, 403(1988), Springer-Verlag, p77-93 （なお、以下において、アルファベット、固有名詞等は原則として英語発音で示す。ただし、明白にその他の外国語と判明しえるもの、例えば後述のドイツ語におけるウムラウトやWeil（フランス人）、Springer書店（ドイツ）等、は当該語にて示す。また、外国語に対応する発音を「かな」で表記するため多少の相違、不正確性がありえる。），池野信一，小山謙二　共著　“現代暗号理論”　電子通信学会発行　１９８６年　等に詳しく述べられている。　以下、有限可換群として有限体を用いた具体例をもとにこの公開鍵暗号を利用した秘密通信の内容を簡単に説明する。なお、有限体上の離散対数問題をＤＬＰと記す。

（有限体上の離散対数問題）ｐを素数、ＧＦ（ｐ）をｐ個の元を持つ有限体（ｐを法とする完全剰余系、なお、ＧＦはガロア体、Galois Fieldの意味）、ｇをその一の原始根（ｇをｐ－１乗してはじめて、その累乗のｐを法とする剰余が１となる正整数）、ａを１≦ａ≦ｐ－１を充たす任意の正整数、αをｐを法とする$g^a$の剰余、すなわち、α≡$g^a$（ｍｏｄ　ｐ）とする。この場合、ｇとｐとａとからαを求めるのは容易であるがｇとｐとαからａを求めるのはｐが大きい素数の場合には大型計算機の発達した今日でも困難である。

【０００４】これは、整数論においては、剰余と原始根と法を与えられた場合に指数を求めることの困難性と言われているものであり、その理由は例えばジー．エッチ．ハーディ及びイー．エム．ライト　著　“アン　イントロダクション　トウ　ザシオリー　オブ　ナンバーズ”　オックスフォードユニバーシティプレス発行（G. H. HARDY &; E. M. WRIGHT著　“ AN INTRODUCTION TO THE THEORY OF NUMBERS ” OXFORD UNIVERSITY PRESS発行），高木貞二　著　“初等整数論講義”　共立出版発行　１９３１年　等にも直接的若しくは間接的に説明されている。

【０００５】次に、図１をもとに、この秘密通信の原理を説明する。公開通信網を使用して相互に秘密通信を行う場合には、あらかじめ公開通信網の提供者が公開鍵と言われる２つの数値ｐとｇとをユーザに公開する。図１においては、より具体的には素数として１１、その原始根として２を選定している。秘密通信を行う二人のユーザＡ、Ｂは各々が１以上ｐ－１以下の秘密鍵と言われる任意の整数ａ、ｂを独立に選定した上で、この数値自身は各自が秘密に保持する。図１においてはａは４、ｂは８である。しかる後、ユーザＡはｐを法とするｇのａ乗の剰余たるα（α≡$g^a$（ｍｏｄ　ｐ））をユーザＢに、ユーザＢはｐを法とするｇのｂ乗の剰余たるβ（β

$\equiv g^{a}$ （ｍｏｄ　ｐ））をユーザＡに知らせ、その上で両者は共有鍵といわれるｐを法とするｇの（ａ×ｂ）乗の剰余たるｋ（$k\equiv g^{a\cdot b}$ （ｍｏｄ　ｐ）を求め、これを第三者には秘密にし、両者のみの秘密通信に使用する。図１においてはαは５、βは３、ｋは４である。

【０００６】

さて、ここに　$k\equiv g^{a\cdot b}$ （ｍｏｄ　ｐ）

$\equiv (g^{a})\cdot{}^{b}$ （ｍｏｄ　ｐ）$\equiv \alpha^{b}$ （ｍｏｄ　ｐ）

$\equiv (g^{b})\cdot{}^{a}$ （ｍｏｄ　ｐ）$\equiv \beta^{a}$ （ｍｏｄ　ｐ）

の関係が成立するため、ユーザＡ、Ｂは各々自己の秘密鍵ａ又はｂと相手から知らされたα若しくはβを使用して容易にｋを計算しえる。しかし、第三者にとっては、秘密鍵ａ、ｂのいずれも知り得ないため、ｐとαとβからｋを計算するのは困難である。

【０００７】このため、ユーザＡ、Ｂはこの共有鍵と言われる数値ｋを使用して両者の秘密通信を行うことが可能となる。その手法を、図２を参照しつつ以下に説明する。現在、有線、無線を問わず、公衆回線を使用した送信は雑音防止、ハード及びソフト的容易性、電子計算機が２進法を採用していること等のため、多くの場合０若しくは１の符号からなるビット情報としてなされる。また、ＡＦ変調等のアナログ信号も、ある単位時間毎に波高をとる等の処理によりディジタル化された上でビット情報とされている。ところで、このビット情報を送信する際、送信情報を何個かずつ区切れば、これらは各々２進法であらわされた整数値とみなせる。従って、情報の送信は$h_1$、$h_2$、…、$h_i$なる２進法の整数値の送信の連続とみなせる。そこで、ユーザＡ、Ｂはあらかじめの別途の取り極め等により、送信は何個かずつに区切られ数値化された情報$h_1$、$h_2$、…、$h_i$毎に両者の共有鍵たるｋを作用させることにより秘密化して送信する。秘密化の手段としては、例えば図２に示すように、①$h_1\times k$、$h_2\times k$、…、$h_i\times k$、②$h_1+k$、$h_2+k$、…、$h_i+k$、③ｈをｋと同じ桁数の数値とした上でｈの各桁の数値（０又は１）を対応するｋの桁の数値が０ならそのまま（０は０のまま、１は１のまま）、１なら逆にする（０なら１とし、１なら０とする）等の攪乱を施す。この秘密化された情報を受信した受信者は、逆の作用をなすことにより復号し、本来の送信されてきた情報を得るものである。この場合、第三者がこの送信情報を盗聴しても、また過誤により第三者に誤送信されたとしても、そして、これらのことは公開通信網を使用する限り多々ありえるのであるが、第三者はユーザＡとユーザＢの共有鍵ｋを知り得ない若しくは知らないため、送信情報を復号するのは困難である。

【０００８】更に、この通信方法は他のユーザ、Ｃ、Ｄ…も各自、１以上ｐ－１以下の任意の整数ｃ、ｄを自己の秘密鍵として保持し、相互に$g^{a\cdot b}$、$g^{a\cdot c}$、$g^{a\cdot d}$、$g^{b\cdot c}$、$g^{b\cdot d}$、$g^{c\cdot d}$…等を共有鍵として公開通信網を使用しての秘密送信をなすことが可能である。このため、ユーザの変更（新規加入、消滅）等にも柔軟に対処できる。更にまた、秘密鍵を定期的に変更する、例えばユーザＡは自己の秘密鍵ａを半年後にａ’に、更に半年後にａ”にというふうに変更することにより、秘密性の一層の増大も図れる。そして、この場合、法となる素数ｐが充分大きければ、各ユーザの秘密鍵が相互に一致する等の不都合も生じ難い。用途も、単なる数値化された文字情報のみならず、ファクシミリ送信のごとく画像情報の秘密送信にも利用しうる。また、公開鍵の作成は公開通信網の提供者に限定されないのも勿論である。また、有料放送においては、放送者が料金を納付した者にのみ放送情報の秘密化に使用したのと逆の作用をなす回路を組み込んだ装置を貸与することにより、料金納付者のみが利用しえる放送をなすことが可能となる。更にまた、長距離用の大型旅客機においては、各座席に復号装置を組み込んだテレビジョンを固定して設け、旅客には映像情報や音声情報を秘密化した上で格納したレーザーディスク、磁気テープ等の可搬式情報記憶体を有料で貸し出すことも問題なく実現可能となる。何故なら、秘密化に使用する共有鍵を、そして当然復号装置と例えばレーザーディスクの秘密化を、旅客機若しくは航空路毎に異なるものとしておけば、レーザーディスクを借り出した旅客による不返還、持ち出し等の盗難防止にも役立つからである。すなわち、レーザーディスクを有料で借り出した旅客は、たとえこのレーザーディスクを返却せずに持ち去ったとしても、座席に固定して設けてある復号装置付きのテレビジョンをも持ち出さない限り他の航空機や航空路ではこの持ち去ったレーザーディスクを利用しえないからである。なお、旅客の持ち出し防止策としてレーザーディスクを、一度でも映像信号を取り出した場合にはこの記憶が自動的に消えさるようにすることも考えられるが、これは旅客サービス低下ととられかねないこと、消去装置を各テレビジョン映像機に装備するのは重量増加となること、飛行機における旅客の機内での返却、新規借り出しのための旅客の通行の原因となり他の旅客の迷惑となること等のため採用は好ましくない。

【０００９】さて、以上の説明でわかるごとく本発明に言う公開鍵暗号通信とは、一般人が通信に容易に接近し得るという条件のもとでの秘密通信、すなわち単なる秘密通信や署名通信に限定されず秘密化された放送や情報源の貸し出しをも含み、更にまた一方向送信のみの通信をも含む概念である。以上、説明したことはあくまでも公開鍵暗号通信方式の原理や基本的応用であり、実際には、例えば、大きな素数そのものをもとめるのは近年の数学の発達のもと比較的容易であるがその原始根をもとめるのは比較的困難であるため可能な限り位数の大きい整数を使用せねばならないこと、送信情報に共有鍵を作用させるに際して必要な処理、演算を可能な限り少なくする必要があること、必要な処理、演算をなす設備から

の制約があること、また、処理、演算の結果増大するビット情報を極力少なくする必要があること、大型計算機の発達と数学特に整数論の応用、例えば分解法則、高次の相互律、素数論、のもとで第三者に復号困難とすること、用途も第三者の詐称を防止するための署名通信等に使用すること等のため種々の改良、変形、応用がなされている。更に、暗号化と復号とで別の鍵を使用すること、別途復号用の鍵を送信する秘密送信の開発、例えば本出願人による特願平３－１９９１４８号、同３－２２７１２５号、同３－３１８８１６号、等もなされている。従って、本明細書にいう共有鍵とは送信情報の暗号化、復号に使用する秘密の数値情報という意味である。更にまた、安全性の確保のため逆に秘密化した情報を解読する試み、上述の例でいうならば、ｐとｇとαとから逆にａをもとめることも研究されている。このため、例えばｐ、ｇをも定期的にかえるだけでなくｐ＋１及びｐ－１は大きな素因数を含むように選定する等の対策もなされている。また、数値化した送信情報と共有鍵による秘密化処理においても種々の研究がなされている。例示した①、②、③の３種の手段のうち、①の手段は必要とする計算量が膨大であり特に共有鍵の桁が増加するとこの欠点は甚だしくなる。一方、②及び③の手段は第三者による復号が①の方法に比較して容易である。このため、必要とする処理量が少なくかつ、解読され難い秘密化も研究されている。更にまた、送信情報がビット化された映像である場合には、有料放送なら無断利用防止の徹底を、レーザーディスク等の有料貸し出しなら貸し出したレーザーディスクをそのまま持ち帰られることの防止の徹底を図るため共有鍵の一部でも不明であるならば復号が困難にすることや、有料放送やレーザーディスクの有料貸し出しに際しての設備面からは復号設備が軽量小型かつ安価であらねばならないこと等、個々の送信情報固有の要請への対応も研究されている。また、ハード的にはビット攪乱器の研究もなされている。これらについては、既述の“現代暗号理論”にも紹介されている。

【００１０】次に、本発明をなすに至ったこれらの技術的背景の説明をも念頭においた上で、離散対数問題の数学的、プログラム的側面について抽象的ではあるが、より一般的に説明する。一般に、有限可換群上の離散対数問題、上記例でいうならばｐを法とする剰余系における指数計算、の困難性に基づく公開鍵暗号通信方式を実現する際の高速性、すなわち暗号化と復号に用する計算等の処理が少なくてすむこと及び安全性、すなわち第三者が通信されている信号そのものを盗聴等により入手したとしてもこれを復号して本来の送信情報を理解することの困難性はこの有限可換群上の離散対数問題若しくは数学的には逆の計算が困難であることに依存する。このため、公開鍵暗号通信方式を高速かつ安全に実現可能な有限可換群上の離散対数問題を構成する技術が必要である。

【００１１】ところで、以上説明した有限体上の離散対数問題は大きな素数ｐとその剰余系のかわりにｑを素数べき、ＧＦ（ｑ）を有限体、ＧＦ（ｑ）の原始根をｇとしてもよいのはあきらかである。このとき、上記問題の困難性の原理はＧＦ（ｑ）の与えられた元ｙに対して、

$y=g^x$　となる整数ｘ（０≦ｘ≦ｑ－１）を求めよというものとなる。

【００１２】有限体上の離散対数問題を第三者の解読が困難なように構成する上で重要なのはｑをｑ－１が１６０桁以上の大きい素数で割れるようにすることである。これは原始根のかわりに使用するこれに近い性質を有する整数としてその位数を大きくすることに相応する。そして、これは計算機等の発達した今日、それほど大きな問題にならない。よって有限体上の離散対数問題は容易に構成できる。しかし、この数学的性質、特に因数についての性質は古くから研究されその結果数々の解法の試みがなされている。そして、次第にその解決に必要な時間が短くなりつつあるのが現状であり、ひいては通信を盗聴等した第三者による復号、すなわち解読が容易になりかねないという問題が生じる。これについてはディ．コッパースミス　“ファストエヴァリューション　オブ　ロガリズムズ　イン　フィールズ　オブ　チャラクタリステック　ツー”，アイイイイ　トランザクション　オン　インフォメーション　シオリー，アイティ３０（１９８４），５８７～５８４頁（D. Coppersmith, “Fastevaluation of logarithms in fields ofcharacteristic two”, IEEE TRANSACTIONS ON IN FORMATION THEORY, IT-30(1984), p587-584）に詳しい。

【００１３】勿論、前述の有限体上の離散対数問題を使用しての秘密通信方法は、送信情報の重要性が解読する手間、費用に比較して高くない場合には充分実用に耐える方法である。なお、有限体の代数学的側面の一般的理論は、抽象的ではあるが、例えばベー；エル．ヴァン　デル　ワルデン　著　“モデルネ　アルゲブラ”　シュプリンガー書店発行　１９３４年（B. L. Van der Waerden 著　“MODERNE ALGEBRA” Springer発行　邦訳「現代代数学」　東京図書発行　１９５９年）に詳しい。

楕円曲線の離散対数問題（ＥＤＬＰ）

有限可換群上の離散対数問題を構成するための第二の方法は、楕円曲線を有限可換群として用いる方法である。これはエヌ．コブリッツ，“ア　コース　インナンバー　シオリー　アンド　クリプトグラフィー”　シュプリンガー書店発行　１９８７年（, N. Koblitz, “A course in number theory andcryptography”, Springer-Verlag, 1987 ）そしてブィ．ミラー，“ユース　オブ　エリプティック　カーブズ　イン　クリプトグラフィー”アドバンシズ　イン　クリプグラフィー　プロシーディングス　オブ　クリプト’８５，レクチャー　ノーツ　イン　コンピュータ　サイエンス，２１８（１９８

６年）　シュプリンガーーフェアラグ，４１７～４２６頁（V. Miller, “Use of ellipticcurves in cryptography”, Advances in Cryptology-Proceedings of Crypto'85, Lecture Notes in Computer Science, 218(1986), Springer-Verlag, p417-426 ）に詳しく述べられている。

【００１４】楕円曲線Ｅ（ＧＦ（ｑ））（ここにＥはａn elliptic curveを意味し、Ｅ（ＧＦ（ｑ））はＥのＧＦ（ｑ）上で定義された有理点の集合の意味である。）上で定義された暗号方式には、現時点ではその安全性の根拠となる楕円曲線上の離散対数問題に上述の有限体上の離散対数問題に対するほど有力な解法がないため、同程度の安全性ならばより簡単、すなわち高速に実現できる。ただし、その数学的内容は高度となる。なお、ここに楕円曲線とは１次元アーベル（Ａｂｅｌ）多様体、あるいは同じことであるが既約で非特異な種数１の射影代数曲線をいい、標数≠２、３の場合（本発明の場合には５以上である）には$Y^2 = X^3 + a \times X + b$で表される。（ここに、ａ、ｂは定義体に属する元）。また、この純粋に数学的な理論の詳細について例えば　志村五郎著“イントロダクション　ツウ　ザアリスメトリック　シオリー　オブ　オートモルフィック　ファンクションズ”（“INTORODUCTION TO THE ARITHEMETRIC THEORY OF AUTOMORPHIC FUCTIONS”）岩波書店、プリンストン大学発行の第４章　エリプティック　カーブズ（CHAPTER 4 ELLIPTIC DURVES），マルチン　アイヒュラー著“アイン　フューリング　イン　ディ　シオリー　デア　アルゲブラッシェン　ツァーレン　ウント　フンクショネン”　ビルクハウザー書店発行　IV章　アルゲブラッシェフンクショネン　イーバー　デン　コンプレクセンツァールケルペル（MARTIN EICHLER著“EINFUEHRLING IN DIE THEORIE DER ALGEBRASCHEN ZAHLENUND FUNKTIONEN” BIRKHAEUSER BERLAG 発行のKAPITEL IV AlgebraischeFunktionen Ueber Den KomplexenZahlkoeper），　志村五郎，谷山豊　共著“近代的整数論”共立出版発行　１９５７年　に詳しい。

【００１５】以下に、本発明に係る秘密通信への応用を考えて、先に説明した素数ｐを法とする有限体上のエルガマル暗号に基づく秘密送信の手順に準じた楕円曲線上の暗号化を考慮の上、その数学的基礎の説明について説明する。なお、図７は楕円曲線を使用した秘密通信の構成を示すものである。

（楕円曲線を使用した秘密通信）

①鍵生成

有限体ＧＦ（ｐ）上定義された楕円曲線Ｅを選ぶ。ここで、ｐは素数である。また、楕円曲線Ｅの有限体ＧＦ（ｐ）の元で構成される群をＥ（ＧＦ（ｐ））と表すことにする。ＧＦ（ｐ）との演算の対応は以下の通りである。

【００１６】

| | |
|---|---|
| ＧＦ（ｐ） | Ｅ（ＧＦ（ｐ）） |
| 単位元は１ | 単位元は無限遠点 |
| 乗法 | 加法 |
| $y = g^x$ | $Y = G + G + \cdots + G$（ｘ個）$= xG$ |
| （ここに、ｙとｇはＧＦ（ｐ）の元、ｘは整数） | （ここに、ＹとＰはＥ（ＧＦ（ｐ））の元、ｘは整数） |
| 乗算は単なるスカラー積 | $G_1$ と$G_2$ は（Ｅ（ＧＦ（ｐ））の元としたときに演算$G_1 + G_2$ は$G_1$ と$G_2$ とを通る直線（$G_1 = G_2$ の場合には$G_1$ におけるＥの接線）とＥとの交点を$G_3$ とした場合、Ｅ上ｘ軸に対し$G_3$ と対称な点$G_3{}'$ と定義される（図３参照）。 |

【００１７】次に$G_1$ をＥ（ＧＦ（ｐ））上の位数の大きな元とする。ここにＧは有限体ＧＦ（ｐ）でのｇの役割を担うものである。この時、ＰとＥ（ＧＦ（ｐ））が

$$Y_B = x_B G_1$$

を計算する。そこで、ユーザＢは$x_B$ を秘密鍵として保持し、$Y_B$ を公開鍵として全ユーザに知らせる。

【００１８】②暗号化

ＡからＢへ平文Ｍを秘密通信する場合を考える。Ａは秘

$$C_1 = kG$$

$$C_2 = M + kY_B$$

ＡはＢに$C_1$ 、$C_2$ を送る。

この暗号方式の公開情報である。このシステムの任意ユーザＢは、任意の整数$x_B$ を選び、Ｅ（ＧＦ（ｐ））上で、

…〔１〕'

密に整数である乱数ｋを選び、自分だけが知っているこの乱数ｋとＢの公開鍵$Y_B$ を用いて次の２組の暗号文$C_1$ 、$C_2$ を作成する。

…〔２〕'

…〔３〕'

【００１９】③復号化

Ｂは自分だけが知っている$x_B$を用いて次式を計算してＭを得る。

$$M + x_B C_1 = C_2 \quad \cdots〔4〕'$$

式〔1〕'、〔2〕'、〔3〕'、〔4〕'のいずれの演算もＥ（ＧＦ（ｐ））上行われ、平文Ｍ、$Y_B$、$G_1$は楕円曲線Ｅ（ＧＦ（ｐ））上の元とする。

【００２０】なお、この場合一次元たる数値情報、上記例でいうなら任意の整数$x_B$と二次元数値情報たる楕円曲線の要素Ｇ（$x_0$、$y_0$），上記でいうなら$Y_B$（$x_0$、$y_0$）との演算については、例えば送信に際して$x_0$若しくは$y_0$から$Y_B$（$x_0$、$y_0$）を求める情報を別途流すと共に$x_0$若しくは$y_0$の一方のみを使用する等の手法が採用される。

【００２１】以上のように、有限体上の元を楕円曲線上の元に、また有限体上の乗法の演算を楕円曲線上の加法の演算に対応させたことにより、暗号方式の形をかえずにその安全性の根拠を、有限体上の離散対数問題から楕円曲線上の離散対数問題に変換することが可能となる。本方式はｐは素数とし、ＧＦ（ｐ）を有限体とし、楕円曲線ＥのＧＦ（ｐ）上の元で生成される群をＥ（ＧＦ（ｐ））とし、Ｅ（ＧＦ（ｐ））の元$G_1$をベースポイントとする。

【００２２】このとき、Ｅ（ＧＦ（ｐ））の与えられた元Ｙに対して、

$Y = x * G_1$

となる整数ｘが存在するならばｘを求めよという問題の困難性に基づく。勿論、これは、$q = p^r$（素数べき）に対し、ＧＦ（ｑ）上のＥについても同様に構成できる。

【００２３】次に述べる理由により上記の楕円曲線上の離散対数問題を公開鍵暗号通信方式へ応用する研究が行われた。

(a) 従来までは、上述の“Fast evaluation of logarithms in fields ofcharacteristic two”の有限体上の離散対数問題の解法のような有力な解法がないため、有限体上の離散対数問題と同程度の安全性ならば、サイズすなわち定義体ＧＦ（ｑ）を小さく取ることができる。このため高速に、すなわち暗号化と復号の処理を少なくできる。

【００２４】(b) 公開鍵暗号通信方式ではその安全性を高めるために、一つの有限可換群の離散対数問題に固定するのではなく定期的に換える必要がある。また、有料放送の場合には受信料の更新等の際にこの問題が生じる。更にまた、レーザーディスクの有料貸し出しの場合には、盗難、持ち去り防止の面から定期的には勿論のこと航空機毎にさえ秘密化を変更したりする必要もある。さて、有限体の場合、一つの素数べきｑに対して有限体は一つしかなく、このため離散対数問題を変更すると暗号化／復号に必要な演算そのものを変更する必要がある。すなわち、ＧＦ（７）の演算では１バイト（８コ）を１ブロックとして扱うと演算に便利であるが、ＧＦ（７）をＧＦ（１７）に変更すると１バイトを１ブロックとして２ブロック単位の演算をなさねばならないというごとく、基本演算（アルゴリズム）をかえねばならない。しかし、楕円曲線の場合、一つの素数べきｑに対して有限体ＧＦ（ｑ）上の楕円曲線Ｅは豊富にあるので、暗号化／復号の演算の基本になる有限体を変えないで楕円曲線Ｅを交換することができる。

【００２５】しかし、楕円曲線上の離散対数問題の構成の場合には、有限体とは異なり使用する楕円曲線ＥのＧＦ（ｑ）の元の個数＃Ｅ（ＧＦ（ｑ））が３０桁以上の大きい素数で割れるように構成することが容易でない。これは＃Ｅ（ＧＦ（ｑ））が簡単に求められないことから起こる問題である。このことに関しては既述の“Acourse in number theory and cryptography”にも述べられている。このため楕円曲線を用いた公開鍵暗号通信方式を構成するには、有限体ＧＦ（ｑ）上の楕円曲線ＥをＥのＧＦ（ｑ）の元の個数＃Ｅ（ＧＦ（ｑ））が大きい素数で割れるように構成することが問題になる。なお、これは従来例の解読対策の１として示したｑ－１が大きい素因数を有することに相応する。

【００２６】次に、公開鍵暗号の安全性の根拠である離散対数問題を定義する有限可換群として適当な楕円曲線を構成する方法として従来例１を説明する。

従来例１

従来例１は、公開鍵暗号の安全性の根拠である離散対数問題を定義する有限可換群としてスーパーシンギュラとよばれる楕円曲線を構成する方法である。図４にこの構成を示す。なお、この構成例は、ア．メネゼス．エス．ヴァンストーン．“ザ　インプレメンテーション　オブ　エリプテック　カーブ　クリプトシステムズ．”アドヴァンセス　イン　クリプトロギ－－プロシーディングス　オブオウスクリプト’９０．レクチャー　ノーツ　イン　コンピューター　サイエンス．４５３（１９９０），シュプリンガー書店．２～１３頁。（A. Menezes,S. Vanstone.“The implemetation of elliptic curve cryptosystems ”,Advances in Cryptology-Proceedings of Auscrypt '90. Lecture Notes inComputer Science. 453(1990). Springer-Verlag. p2-13 ）に詳しく述べられている。

【００２７】以下同図に沿い、スーパーシンギュラとよばれる楕円曲線の構成法を

①楕円曲線の候補の決定、

②適当な拡大次数ｍの決定、

③実際の楕円曲線の構成例に分けて説明する。

①楕円曲線の候補の決定

次の三個のＧＦ（２）を定義体にもつスーパーシンギュラ楕円曲線を考える。

【００２８】$E_1 : y^2 + y = x^3 + x + 1$

$E_2$ ：$y^2+y=x^3+x$

$E_3$ ：$y^2+y=x^3$

各楕円曲線 $E_i$ のＧＦ（$2^m$）上の元で構成される群 $E_i$（ＧＦ（$2^m$））とは次のような群である（ｉ＝１～３）。

【００２９】

$$E_1(GF(2^m))=\{x,y\in GF(2^m)\mid y^2+y=x^3+x+1\}\cup\{\infty\}$$

$$E_2(GF(2^m))=\{x,y\in GF(2^m)\mid y^2+y=x^3+x\}\cup\{\infty\}$$

$$E_3(GF(2^m))=\{x,y\in GF(2^m)\mid y^2+y=x^3\}\cup\{\infty\}$$

ここで∞は無限遠点を表す。このとき各 $E_i$（ＧＦ（$2^m$））には先に説明したごとく加法が定義され、∞が零元となる有限可換群になる。また、各群の元の個数 $\#E_i$（ＧＦ（$2^m$））は一般の場合には計算が困難であるがかかる条件のもとでｍが奇数のとき次のようになる（ｉ＝１～３）。なお、この理由はジェイ．エッチ．シルバーマン“ザアリスメトリック オブ エリプティック カーブズ”ジーティーエム１０６，シュプリンガーーフェアラグ ニューヨーク １９８６年（J. H. Silverman"The Arithmetic of Elliptic Curves" GTM106, Springer-Verlag New York1986 ）に詳しい。

【００３０】

$$\#E_1(GF(2^m))\quad 2^m+1-2^{(m+1)/2}\ \text{in case}(m\equiv 1,7 \pmod 8)$$
$$\qquad\qquad 2^m+1+2^{(m+1)/2}\ \text{in case}(m\equiv 3,5 \pmod 8)$$
$$\#E_2(GF(2^m))\quad 2^m+1+2^{(m+1)/2}\ \text{in case}(m\equiv 1,7 \pmod 8)$$
$$\qquad\qquad 2^m+1-2^{(m+1)/2}\ \text{in case}(m\equiv 3,5 \pmod 8)$$
$$\#E_3(GF(2^m))=2^m+1$$

②適当な拡大次数ｍの決定

公開鍵暗号の安全性の根拠となる上述の楕円曲線の離散対数問題はベースポイントである元Ｐの位数が３０桁以上の大きな素数で割れなければ簡単に解けることが知られている。なお、このことは先に示した有限体ＧＦ（ｑ）の離散対数問題において、ｑ－１が大きな素因数を持つことに相応するものである。そして、この解法についてはエス．シー．ポーリング アンド エム．イー．ヘルマン，“アンインプルーブド アルゴリズム フォ コンピュティング ロガリズムズオーバー ＧＦ（Ｐ） アンド イッツ クリプトグラフィック シグニフィカンス”，アイイイイ トランザクション オン インフォーメーション シオリー．アイティー２４ １９７８年．１０６～１１０頁（S. C. Pohlig and M. E. Hellman, “An improved alogorithm for computing logarithms over GF(p)and its cryptographic significance ”, IEEE TRANSACTION ON INFORMATIONTHEORY, IT-24(1978),p106-110）に詳しい。ところで、そのような元Ｐが存在するための必要十分条件はＥ（ＧＦ（ｑ））の元の個数が大きな素数で割れることである。

【００３１】そこで、（１）に述べた楕円曲線 $E_i$ についてその元の個数 $\#E_i$（ＧＦ（$2^m$））が大きな素数で割れるようにｍを求める。（ｉ＝１～３）

③実際の楕円曲線の構成例

楕円曲線 $E_3$ のＧＦ（$2^m$）上の元で構成される群 $E_3$（ＧＦ（$2^m$））の元の個数の素因数分解を行った結果

ｍ＝１９１のとき、$\#E_3(GF(2^m))=2^{191}+1=3*p_1$

ｍ＝２５１のとき、$\#E_3(GF(2^m))=2^{251}+1=3*238451*p_2$

（$p_1$、$p_2$ は素数）

となることがわかった。なお、$p_1$、$p_2$ が素数であることは、各々２のべき乗の因数であること、またこのため特殊な形であらわされること（例えば $2^{191}+1$ 及び $2^{251}+1$ の素因数は各々必ず２・１９１・ｍ＋１、２・２５１・ｍ＋１の形となる。）、その他マシマ．コンピュ．，４２，１６５，２９７～３３０頁，１９８４年１月号（Math. Comp., 42, 165, pp. 297～330(Jan. 1984) にてエッチ．コーエン 及び エッチ．ダブリュ．レンストラ（H. Cohen and H. W.Lenstra ）が紹介している方法等により今日では検証可能である。

【００３２】よって $E_3$（ＧＦ（$2^{191}$））上の位数が素数 $p_1$ となる元をベースポイントＰとする楕円曲線上の離散対数問題もしくは $E_3$（ＧＦ（$2^{251}$））上の位数が素数 $p_2$ となる元をベースポイントＰとする楕円曲線上の離散対数問題を安全性の根拠にした公開鍵暗号通信方式を構成すればよいことが結論づけられる。なお、ここにベースポイントとは、従来例で示した原始根ｇに相応した役割を担うものである。

【００３３】

【発明が解決しようとする課題】しかし１９９１年になって楕円曲線上の離散対数問題を群同型を通じて有限体上の離散対数問題に帰着させて解く解法が提案された。この解法は特に、スーパーシンギュラと呼ばれる楕円曲線上の離散対数問題については高々楕円曲線の定義体ＧＦ（ｑ）の６次拡大体ＧＦ（$q^6$）上の有限体上の離散対数問題と同等になる。第一の従来例は十分な安全性を確保できないことがわかった。以後この解法を帰着法と呼ぶ。なお、スーパーシンギュラについては、後に説明する。

【００３４】そこでまず帰着法について簡単に説明する。これはア．メネゼス，エス．ヴァンストーン 及びティー．オカモト，“リデュウーシング エリプティックカーブ ロガリズムズ ツウ ロガリズムズ インアフィン フィールド”，プロシーディングス オブ

ザ　２２回　アニュアル　エイシーエム　シンポジュウム　オン　ザ　シオリー　オブ　コンピューティング，１９９１年　８０～８９頁（A. Menezes, S. Vanstone and T. Okamoto, “Reducing elliptic curvelogarithms to logarithms in a finite field”, Proceedings of the 22ndAnnual ACM Symposium on the Theory of Computing, 1991, P80-89 ）に詳しく述べられている。

【００３５】帰着法の基本は、数学特に代数幾何学若しくは代数的整数論の理論、具体的にはヴェイユ対（Weil pairing）を使用するものである。ここに、帰着法を純数学的に説明すると以下のようになる。なお、この際使用する元、同型、体、環、群等の意味や純数学的理論及びそれらの数学的記号は前掲の“現代代数学”の他　日本数学会編集　“数学辞典”岩波書店発行　１９８５年等に、また後で説明する本発明に関係する純数学的、特に整数論の理論は前掲の“初等整数論講義”や“THEORY OF NUBERERS”の他に、同じく前掲のJ. H. Silverman 著　“The Arithmetic of Elliptic Curves”に詳しい。

【００３６】ｑを素数べきｐ$^r$ として、有限体ＧＦ（ｑ）上定義された楕円曲線をＥとし、ＥのＧＦ（ｑ）上の元で構成される群をＥ（ＧＦ（ｑ））とする。楕円曲線には、ヴェイユ対（Weil-pairing）が存在する。このヴェイユ対とは、以下のようなものである。

【００３７】（ヴェイユ対）ｎを正整数とし、ｐと互に素、すなわち（ｎ，ｐ）＝１とする。

・ＥをＧＦ（ｑ）上定義された楕円曲線としＥ［ｎ］＝｛Ｅ∋Ｐ　｜　ｎＰ＝∞｝とする。（ここに｛　｝は集合を意味する。）

（＃Ｅ［ｎ］＝ｎ$^2$ でＥ［ｎ］はμ／ｎμ×μ／ｎμに群同型である。）このとき、ヴェイユ対　ｅｎとはＥ［ｎ］×Ｅ［ｎ］から１のｎ乗根μｎへの写像（map）　　ｅｎ：Ｅ［ｎ］×Ｅ［ｎ］→　μｎ　　であり、次の性質を満たす。

【００３８】

(a) 双線形（Bilinear）

$$e_n(S_1+S_2,\ T)=e_n(S_1,\ T)\,e_n(S_2,\ T)$$

$$e_n(S,\ T_1+T_2)=e_n(S,\ T_1)\,e_n(S_1,\ T_2)$$

(b) 恒等写像（Identity）

すべてのＴ∈Ｅ［ｎ］なるＴに対しｅｎ（Ｔ，Ｔ）＝１

(c) 交代（Alternating ）

ｅｎ（Ｓ，Ｔ）＝ｅｎ（Ｔ，Ｓ）$^{-1}$

(d) 非退化（non degenerate）

もし、全てのＳ∈Ｅ［ｎ］なるＳに対しｅｎ（Ｓ，Ｔ）＝１ならば、

Ｔ＝∞

以上の性質を用いて、ヴェイユ対　ｅｎは以下の関係を満たすのがわかる。

【００３９】Ｅ［ｎ］＝〈Ｓ〉×〈Ｔ〉とする。

１．このとき、ｅｎ（Ｓ，Ｔ）は１の原始ｎ乗根である。（何故ならば、ｅｎ（Ｓ，Ｔ）$^d$ ＝１　ならばｎはｄの因数、すなわちｎ｜ｄ　である。）

∵ｅｎ（Ｓ，Ｔ）$^d$ ＝１とする。

【００４０】このとき、性質(a) により、

ｅｎ（［ｄ］Ｓ，Ｔ）＝１

一方、Ｅ［ｎ］の任意の元は［ｘ］Ｓ＋［ｙ］Ｔと表されるので、

$$\begin{aligned}e_n([d]S,\ [x]S+[y]T)&=e_n([d]S,\ [x]S)\cdot e_n([d]S,\ [y]T)\\&=e_n([d]S,\ T)^y\\&=1\end{aligned}$$

（∵　(a)，(b)）

となる。

となるので性質(d) より

［ｄ］Ｓ＝０

よって、

ｎ｜ｄ

２．ｅｎは、Ｅ［ｎ］の部分群〈Ｓ〉とμｎの群同型を与える。

【００４１】

$$\begin{aligned}\phi: E[n]\supset\langle S\rangle &\longrightarrow \mu_n\\ lS\ (\in\langle S\rangle) &\longrightarrow e_n(lS,\ T)\end{aligned}$$

・群準同型は明らか

・全射、単射も成立する。

なお、ミラーによりヴェイユ対は確率的多項式時間で計算できることが示されている。

【００４２】次に、有限体ＧＦ（ｑ）の高々ｎ次拡大体ＧＦ（ｑ$^n$ ）に１のｎ乗根μｎは含まれる。

従って、ヴェイユ対は　　$\phi:\langle S\rangle \longleftrightarrow GF(q)$

という準同型φを与える。そこで、このヴェイユ対を用いて、ＥＤＬＰがどのようにして帰着法により解法されるかを述べる。

（算法（Algorithm））

入力：Ｐ∈Ｅ（ＧＦ（ｑ））を位数（order ）ｎの元とする。更に〈Ｐ〉∋Ｒを取る。出力：Ｒ＝ｌＰなる整数ｌ

（１）ＧＦ（ｑ$^k$ ）⊃μｍなる最小の正整数ｋをみつける。

（２）Ｅ［ｎ］∋Ｑを、Ｅ［ｎ］＝〈Ｐ〉×〈Ｑ〉とな

るように取る。

（３）上記準同型$\phi$による中への準同型

$\phi$：〈P〉 ⟶ $\mu n \subset GF(q^k)$

ＩＰ ⟶ en（ＩＰ，Ｑ）

により、〈P〉を有限体ＧＦ（$q^k$）の中に埋め込む。

【００４３】$\beta = \phi(R) = en(R, Q)$

$\alpha = \phi(P) = en(P, Q)$

（４）ＧＦ（$q^k$）での離散対数問題　$\beta = \alpha^{l'}$を解く。（ここにｌ’は正確にはｌ’）。

（５）ｌ＝ｌ’を出力

この算法の問題は、（１）と（２）である。（（３）の有限体への埋め込みは前述のごとくミラーにより確率的多項式時間で可能）

（２）ついて、Ｅ［ｎ］＝〈P〉×〈Q〉　〈＝〉　en（P，Q）が１の原始ｎ乗根より、Ｑを繰り返し取る回数Φ（ｎ）／ｎはメルテンス（Mertens ）の第３定理より≦６　loglog　ｎになる。（ここにΦ（ｎ）はオイラー（Euler ）の関数であり、ｎと互いに素かつｎ以下の正整数の総個数をあらわす。）又、en（P，Q）の検査は、確率的多項式時間で可能なので、（２）は、確率的多項式時間で可能になる。

【００４４】故に問題は（１）である。この（１）に関して、Ｅがスーパーシンギュラーになる場合について、

Ｒ≦６

であり、Ｅに対して、ｋが表で与えられる。一方、否スーパーシンギュラーに関しては、このような対応表はないが、仮に、　ＧＦ（$q^k$）⊃$\mu n$　ここに、ｋは十分小　となれば、スーパーシンギュラーな場合と、何らかわりなく解けることがわかる。

【００４５】更に、ＳＣＩＳ９１で静谷－桜井－岡本らの発表したＥＤＬＰが、構造的計算量理論の観点から、ＦＤＬＰと同じクラスＮＰ∩Ｃｏ－ＮＰに入ることが証明されたが、これも又、上述のアルゴリズムが成立することから証明された。このためＥ（ＧＦ（ｑ）∋Ｐをベースとする楕円曲線上の離散対数問題は、Ｐの位数とｑが互いに素なときには、有限体ＧＦ（ｑ）のある拡大体ＧＦ（$q^r$）上の離散対数問題に帰着して解くことができる。

【００４６】特にＥがスーパーシンギュラと呼ばれる楕円曲線（ＥＤＬＰ）の場合には有限体ＧＦ（ｑ）の高々６次拡大体ＧＦ（$q^6$）上の離散対数問題（ＤＬＰ）に帰着される。従来例１はスーパーシンギュラーとよばれる楕円曲線を構成している。この為、安全性の根本である楕円曲線上の離散対数問題に帰着法を適用すると、$E_3$（ＧＦ（$2^n$））上の離散対数問題は有限体ＧＦ（$2^{2n}$）上の離散対数問題と同程度の難しさ、すなわち解く方からみればそれだけ容易、になる。ところで、上述のように数学、特に整数論の応用、ひいてはその解読の研究及び大型計算機の発達のもと、現時点では有限体ＧＦ（$2^{2n}$）上の離散対数問題は２ｎが５１６ビット以上なければ十分な安全性を確保できないといわれている。これについては、既述の“Fast evaluation of logarithms in fields of characteristic two ”に詳しく述べられている。よって、従来のままでは楕円曲線Ｅの定義体である有限体ＧＦ（$2^n$）のｎを２５６以上の数にしなければならないこととなる。一方２５６以上のｎを取ると安全性は確保されるが、暗号化、復号のための処理が多くなり、大容量計算機を使用する場合はもちろんハード面に制約がある場合は特に、高速送信や人の視覚に相応しての画像情報の再生が難しくなる。

【００４７】また、ＧＦ（２）上の楕円曲線を拡大体ＧＦ（$2^n$）に持ち上げる、すなわちＧＦ（２）上の楕円曲線をＧＦ（$2^n$）の楕円曲線とみるという方法で公開鍵暗号に用いる楕円曲線を構成するため、ｎビットの大きさの定義体上の提供できる楕円曲線の個数はＧＦ（２）上のスーパーシンギュラの楕円曲線の個数と同じ個数、つまり３個しかない。さらにこの方法では、楕円曲線ＥのＧＦ（$2^n$）の元の個数＃Ｅ（ＧＦ（$2^n$））が３０桁以上の大きい素数で割れるようにするために＃Ｅ（ＧＦ（$2^n$））の素因数分解が必要であるが、素因数分解はｎが大きくなると必要な計算量が指数関数的に増大し、このため非常に時間がかかる。ひいては、公開鍵を提供する側にも困難が生じる。

【００４８】従来例２

次に帰着法を考慮して構成された楕円曲線の構成法を従来例２として説明する。これは、公開鍵暗号通信方式の安全性の根拠である離散対数問題を定義する有限可換群としてスーパーシンギュラでない楕円曲線を構成する方法である。図５にこの構成を示す。なお、この構成例は、ティー．ベス，エフ．シャッファー共著　“ノンスーパーシンギュラー　エリプティック　カーブズ　フォー　パブリック　キー　クリプトシステムズ”，アドバンシズ　イン　クリプトロギー－プロシーディングス　オブ　ユーロクリプト’９１，レクチャー　ノーツ　インコンピューター　サイエンス，５４７（１９９１年），３１６～３２７頁，（T.Beth.&: F. Schaefer. “Non supersingular elliptic curves for public key cryptosystems”, Advances in Cryptology-Proceedings of Eurocrypt '91,Lecture Notes in Computer Science, 547(1991), p316-327）に詳しく述べられている。

【００４９】以下同図に沿い、この従来例２の構成法を、①楕円曲線の候補の決定、②適当な拡大次数ｍの決定、③実際の楕円曲線の構成例に分けて説明する。

①楕円曲線の候補の決定

有限体ＧＦ（２）を選ぶ。次の二つの有限体ＧＦ（２）上のスーパーシンギュラでない楕円曲線を考える。

【００５０】$E_4 : y^2 + xy = x^3 + x^2 + 1$

$E_5 : y^2 + xy = x^3 + 1$

各楕円曲線$E_i$のＧＦ（$2^m$）上の元で構成される群$E_i$（ＧＦ（$2^m$））の元の個数＃$E_i$（ＧＦ（$2^m$））

は次のようになる。（ｉ＝４、５）。

$$\#E_4\ (GF(2^m)) = 1+2^r - \{(1+(-7)^{1/2})/2\}^m - \{(1-(-7)^{1/2})/2\}^m$$

$$\#E_5\ (GF(2^m)) = 1+2^r - \{(-1+(-7)^{1/2})/2\}^m - \{(-1-(-7)^{1/2})/2\}$$

②適当な拡大次数ｍの決定

各楕円曲線$E_i$について拡大次数ｍを次の２条件を満たすようにとる。（ｉ＝４、５）

〔条件１〕楕円曲線$E_i$についてその元の個数＃$E_i$（ＧＦ（$2^m$））が大きな素数で割れる（ｉ＝４、５）。

〔条件２〕楕円曲線$E_i$についてその元の個数＃$E_i$（ＧＦ（$2^m$））の最大の素因数をｐとし十分大きい正整数をｔとするとき、ｔ以下の任意の正整数ｋに対して$2^{mk}-1$はｐを素因数にもたない（ｉ＝４、５）。

【００５１】〔条件２〕は帰着法により$E_i$（ＧＦ（$2^m$））上の離散対数問題を有限体ＧＦ（$2^m$）の拡大体に帰着させるときに、その拡大次数がｔ以上になることを意味する。勿論ｔが大きければそれだけ安全性が高くなる。

③実際の楕円曲線の構成例

楕円曲線$E_4$のＧＦ（$2^m$）上の元で構成される群$E_4$（ＧＦ（$2^m$））の元の個数の素因数分解を行った結果ｍ＝１０７のとき、＃$E_4$（ＧＦ（$2^m$））＝２＊素数$p_3$

となることがわかった。更にｋ＝１～６に対して$2^{mk}-1$は素数$p_3$を素因数にもたないことが計算機で求められる。

【００５２】よって$E_4$（ＧＦ（$2^{107}$））上の位数が素数$p_3$となる元をベースポイントＰとする楕円曲線上の離散対数問題の困難さを安全性の根拠にした公開鍵暗号を構成すればよいことが結論づけられる。従来例２の構成の楕円曲線は〔条件２〕を満たすので、安全性の根拠を依存させる楕円曲線上の離散対数問題を有限体上の離散対数問題に帰着させる帰着法による解法よりも既述の“An improved alogorithm for computing logarithmsover GF(p) and its cryptographic significance ”の解法の方が強力なため、有限体ＧＦ（$2^n$）のｎを１００以上の数にすれば十分な安全性が確保されることがわかる。しかし計算機の進歩に従って次第にこのｎは大きくなると考えられ、ｎが大きくなると、暗号化、復号のために必要な処理が増大しこのため高速に実現することが難しい。

【００５３】また従来例１と同様、ＧＦ（２）上の楕円曲線を拡大体ＧＦ（$2^n$）に持ち上げる、すなわちＧＦ（２）上の楕円曲線をＧＦ（$2^n$）上の楕円曲線とみるという方法で公開鍵暗号に用いる楕円曲線を構成するため、ｎビットの大きさの定義体上の提供できる楕円曲線の個数はＧＦ（２）上のスーパーシンギュラでない楕円曲線の個数と同じ個数、つまり２個しかないという欠点がある。さらにこの方法は、楕円曲線ＥのＧＦ（$2^n$）の元の個数＃Ｅ（ＧＦ（$2^n$））が３０桁以上の大きい素数で割れるようにするために＃Ｅ（ＧＦ（$2^n$））の素因数分解を必要とするが、素因数分解はｎが大きな場合には急速に困難となる。

【００５４】本発明は、以上説明した従来例における技術的背景及び技術的問題の下で

①楕円曲線上の離散対数問題の解法に帰着法が適用できない。

②同じビット数の定義体上の楕円曲線を豊富に提供できる。

③更に、上記①及び②を充たす楕円曲線を容易に作成可能である。

という特徴を持つ楕円曲線を用いた公開鍵暗号通信方式を提供することを目的としてなされたものである。

【００５５】

【課題を解決するための手段】上記目的を達成するために、請求項１の発明においては、数値化した通信文をＥ（ＧＦ（ｐ））の元と演算をなすことにより秘密通信若しくは署名通信を実現する公開鍵暗号通信方式において、ｐを素数とし、有限体ＧＦ（ｐ）を定義体にもつ楕円曲線ＥのＧＦ（ｐ）上の元で構成される群をＥ（ＧＦ（ｐ））とするとき、Ｅ（ＧＦ（ｐ））の元の個数がｐになるように楕円曲線Ｅをとり、前記Ｅ（ＧＦ（ｐ））上定義される離散対数問題の困難さを公開鍵暗号通信方式の安全性の根拠にもつことを特徴としている。

【００５６】請求項２の発明においては、請求項１の発明において、ＧＦ（ｐ）を定義体にもつ楕円曲線Ｅは、正整数ｄを、虚二次体Ｑ（（－ｄ）$^{1/2}$）の類数が小さくなるようにとり、素数ｐを、４＊ｐ－１＝ｄ＊平方数の関係を充たすようにとり、ｄにより定まる類多項式$H_d$（ｘ）＝０のｐを法とした解をｊ不変数にもつようにして得られることを特徴としている。

【００５７】請求項３の発明においては、請求項２の発明において、虚二次体Ｑ（（－ｄ）$^{1/2}$）の類数が１であることを特徴としている。

【００５８】

【作用】請求項１及び請求項２の発明においては、帰着法の適用されない楕円曲線を使用することとなるため、楕円曲線の定義体ＧＦ（ｐ）が小さくできる。請求項３の発明においては、虚二次体Ｑ（（－ｄ）$^{1/2}$）の類数が１であるため、請求項１及び請求項２の発明の実施に必要な楕円曲線の作成が容易となる。

【００５９】

【実施例】以下、本発明を実施例に基づき説明する。これに先立ち、本発明に係る楕円曲線そのものの作成方法と理論的基礎につき説明する。

（楕円曲線の作成）Ｐを素数とし、有限体ＧＦ（ｐ）上の楕円曲線ＥのＧＦ（ｐ）の元で構成される群をＥ（Ｇ

F（p））とするとき、E（GF（p））の元の個数がGF（p）の標数と互いに素でないように、つまりpになるように楕円曲線Eをとる。そして、このような楕円曲線は少なくとも各素数に対して1個存在するため、前述の第（2）の目的も達成される。

【0060】また、有限体GF（p）上の楕円曲線EのGF（p）の元で構成される群をE（GF（p））とするとき、E（GF（p））の元の個数がpになるようなEは次のようにして構成する。5以上の正整数dを、前述の第（3）の目的を達成すべくその類多項式$H_d$（X）の構成が容易であるように虚二次体Q（（－d）$^{1/2}$）の類数が（イデアル類の個数）が小さい整数とし、素数pを、4＊p－1＝d＊平方数となるようにとると、求めるGF（p）上の楕円曲線Eのj不変数は、dにより定まる類多項式$H_d$（X）＝0のpを法とした解$j_0$により与えられる。

【0061】上記$j_0$をj不変数にもつ有限体GF（p）上の楕円曲線はGF（p）上同型を同一視すると次の2つになる。

$E_0$：$y^2=x^3+c^2\times a\times x+c^3\times a$（cはGF（p）の平方非剰余）

$E_1$：$y^2=x^3+a\times x+a$

$a=j_0$／（1728－$j_0$）

このうちp個の元をもつ楕円曲線は、

$E_1$（GF（p））∋$X_1$、$E_0$（GF（p））∋$X_0$

をとり、それぞれをp倍したとき零元になるほうである。

（帰着法が適用できない楕円曲線の作成）

1．存在について、先述の帰着法によりE（GF（q））の離散対数問題が解かれるのを防ぐには、

E（GF（p））∋P≠0 を pP＝∞

となるようにGF（p）上で定義された楕円曲線E／GF（p）を取り、さらに離散対数問題のベース点（有限体での原始根に対応する点）にp-ねじり率（torsion）点（p倍すると∞になる点）Pを取るとよい。このとき、帰着法に必要な〈P〉と有限体との準同型φはヴェイユ対$e_p$がないので構成できない。

【0062】なお、ハッセ（Hasse）の定理により、E（GF（p））の元の個数には以下の制限がある。

$$|\#E(GF(p))-p-1| < 2\sqrt{p} \quad \cdots(1)$$

つまり、＃E（GF（p））の取れ得る範囲は、

$$q+1-2\sqrt{p} < \#E(GF(p)) < p+1+2\sqrt{p} \quad \cdots(2)$$

である。

【0063】ここで、E（GF（p））がp-torsion を含む必要条件である

＃E（GF（p））≡0 （mod p）

は、上記の範囲に属していることがわかる。（つまり、＃E（GF（p））＝npとなる可能性がある。）更に、素体上の楕円曲線に関しては、次のドイーリング(Deuring)の定理が成立する。

【0064】＃E（GF（p））＝p＋1－apを表すと、上記ハッセの定理（1）は

$$|ap| < 2\sqrt{p} \quad \cdots(3)$$

と表されるが、この（3）式を満たす任意の整数apに対して、d＝ap$^2$－4pとおくと、GF（p）上の代数曲線で元の個数がp＋1－apとなる楕円曲線が、Q（$\sqrt{d}$）の類数（イデヤル数の個数）個存在する。

【0065】なお、類数に関しては表があるため、dに対応して容易に求められる。又、類数は1以上なので、上記（1）式を充たすGF（p）上の楕円曲線が常に存在することもわかる。

2．作成について次に代数曲線の作成法について説明する。

【0066】帰着法は、E（GF（q））∋Qの0（Q）＝nとするとき、

（n，p）≠1

でなければ適用できない。これは、準同型φが構成できないからである。ところで、今までの楕円曲線の離散対数問題の解法は常にベースポイントの位数がpと互いに素であることを仮定している。

【0067】しかし、例えば、q＝2$^r$とし E（GF（q））∋p、O（p）＝2$^l$・t（（2，t）＝1）なる元pをベースポイントとしたときの解法は、次のようになる。

（問題 ※）

Q＝xPなるxを求めよ。

（解法）

$e_A$ t：E［2$^l$ t］×E［2$^l$ t］⟶ $\mu_{At}$＝｛1の2$^l$ t乗根｝となるヴェイユ対は存在しない（eとμの下添え字のAは2$^l$）。

【0068】そこで、〈2$^l$ P〉上の離散対数問題を考える。

2$^l$ P＝P'

2$^l$ Q＝Q' とし、まず、Q'＝x' P' なるx'を求める。ここで、o（P'）＝t （t，2）＝1より、ヴェイユ対$e_t$が存在する。

$e_t$：E［t］×E［t］⟶$\mu_t$＝｛1のI乗根｝⊂GF（$q^k$）

（GF（$q^k$）はGF（q）のk次拡大体）

よって、x'は有限体上の離散対数問題を解くことにより求められる。

【0069】o（Q－x' P）＝2$^l$より

Q－x' P∈〈tP〉

故に、

s・tP＝Q－x' P

なるｓ∈｛１、…、$2^l-1$｝を求める。

【００７０】これは、小さい素数巾の離散対数問題を解くことになるので、容易になしえる。これは前述の"An improved algorithm for computing logarithms over GF(p)and its cryptographic significance"に詳しい。

Ｑ＝（ｓｔ＋ｘ’）Ｐ　を得る。

よって、帰着法を拡張して解くことができる。（ヴェイユ対を使用した解法が、適用できない楕円曲線について）

楕円曲線の離散対数問題

Ｅ（ＧＦ（ｑ））∋Ｐと〈Ｐ〉∋Ｑが与えられた時

ｘＰ＝Ｑ　　となるＱを求める（$q=p^r$）

解法

ｏ（Ｐ）＝ｎとおく。

１．（ｎ，ｐ）＝１のとき、ヴェイユ対による解法により有限対上の離散対数問題

２．（ｎ，ｐ）＝ｐのとき

$n=p^K l$ とおく　　（（ｌ，ｐ）＝１）

$$|\#E(GF(p))-p-1| \leqq 2\sqrt{p}$$

$$\therefore p+1-2\sqrt{p} \leqq \#E(GF(p)) \leqq p+1+2\sqrt{p}$$

である。そこで、ｎ＝ｐｌよりｌの可能性を考える。（なお、Ｋ＝１となるのはハッセの定理より明白）ｌ＝２としてみる。

【００７３】$2p \leqq p+1+2\sqrt{p}$

$p-1 \leqq 2\sqrt{p}$

$p^2-2p+1-4p \leqq 0$

$p \leqq 3+\sqrt{(9-1)}=3+2\sqrt{2}$

$p \leqq 5$

従って、ｐが大きい素数のときｌ＝１である。

すなわち、　＃Ｅ（ＧＦ（ｐ））＝ｐ

２－２．　ｌ＝１のとき

２－１より、素体ＧＦ（ｐ）上の楕円曲線での暗号を考えるとき

＃Ｅ（ＧＦ（ｐ））＝ｐ　　のときのみ、適当な解法がないことがわかる。従って、以後　＃Ｅ（ＧＦ（ｐ））＝ｐとなる対数曲線の構成を考えるとよい。（帰着法の通用しない楕円曲線の構成）以上説明したことをまとめると、以下のようになる。

【００７４】ｐ：素数

ＧＦ（ｐ）：ｐ個の元をもつ有限体・

Ｅ／ＧＦ（ｐ）：ＧＦ（ｐ）上定義された　＃Ｅ（ＧＦ（ｐ））＝ｐ　となる楕円曲線。

$G_1$：Ｅ（ＧＦ（ｐ））の任意の∞でない元（ベースポイント）

（Ｅ（ＧＦ（ｐ））, $G_1$）によるＥＤＬＰとは、Ｅ（Ｆｐ）∋Ｑに対して　$Q=xG_1$　なるｘをみつける。この場合、いわゆるしらみつぶしで全ケースをあたるしか解法がないため、計算機の発達した今日でも素数ｐが十分大きければ、実用上可能な解法がないこととなる。

２－１．　ｌ≠１　のとき

先述の方法、（問題　※）の解法に従って〈$p^K P$〉の離散対数問題を解く。

【００７１】$p^k Q=x' p^K P$

次に同様に先述の方法、（問題　※）の解法に従って

$Q-x'P=i'lP$　　　$i=0,\cdots,p^K-1$

なるｉを求める。ここで、ＥＤＬＰはまずｎが大きい素数で割れなければ、全ケースのしらみつぶしによる解法、いわゆる絨緞爆撃、がなされてしまう。従って、ｐが大きい素数でなければならない。ｌが大きい素数のとき、ｐは小さい素数となるが、実際に暗号に用いる有限体ＧＦ（ｑ）はｐ＝２かｐは大きい整数に限られてくるのでｐ＝２としてよい。この場合、ｌがなるべく大きい素数をもつようにＥはとられているので充分、この解法で解けてしまう。

【００７２】・ｐが大きい素数のとき、上述の理由と同様の理由で有限体はＧＦ（ｐ）を考えてよい。このとき、ハッセの定理より

実施例１

図６は本発明に係る楕円曲線を用いた公開鍵暗号通信方式の一実施例の構成法を示すものである。

【００７５】以下本図を参照しながら実施例の手順を、①正整数ｄの決定ステップ、②素数ｐの生成ステップ、③類多項式$H_d$（ｘ）のｐを法とした解を求めるステップ、④楕円曲線Ｅの決定ステップに分けて説明する。また以下で用いられる虚二次体及び類数（イデアルの数）に関してはエス・ラング　著　“アルゲブラック　ナンバー　シオリー”，ジーティーエム１１０，シュプリンガー書店発行，ニューヨーク　１９８６年　(S. Lang, “Algebraic number theory ”, GTM110, Springer-Verlag, New York, 1986 ）に、類多項式及びｊ不変数に関しては、エス．ラング，“エリプティック　ファンクションズ”，アディソンーウエスレイ１９７３年（S. Lang, “Elliptic functions”, Addison-Wesley, 1973）に詳しい。

【００７６】①正整数ｄの決定ステップ

正整数ｄを、虚二次体Ｑ（$(-d)^{1/2}$）の類数が小さくなるようにとる。ここでは、かかる正整数のうち類数が１の整数の中で１９をｄとする。これは、次の素数ｐを求めるステップでの計算が楽なことによる。（なお、類数が１の虚二次体をつくる正整数としては他に、１、２、３、７、１１、４３、６７、１６３の９個があり、類数２の虚二次体をつくる正整数には１０、１５、２６、３０等がある。そしてこれらはディリクレー、デデキント著　酒井孝一訳及び追記“整数論講義”　共立出版刊に表として掲載されているのをはじめとして、二次体に関する整数論を記載した多数の本に記されている。ただし、これら全ての整数が本発明の実施に適当とは限

らない。すなわち、例えば、１、２、７の場合には４＊ｐ－１＝ｄ＊平方数　を充たす素数が存在しない。）

②素数ｐの生成ステップ

素数ｐを、４＊ｐ－１＝ｄ＊平方数となるようにとる。ここでは、

ｐ＝235208607464683519348918416 23

ととると、

$4 * p - 1 = 19 * (1451 * 48496722383)^2$

となるので条件を満たす。（なお、３０桁程度の素数そのものは容易に求められる。このためかかる４＊ｐ－１＝ｄ＊平方数　という条件を充たす素数は、試行錯誤法ではあるが容易に発見可能である。また、古くからの実際の計算や近年の解析的整数論におけるブルン（Brun）やセルベリ（Selberg ）のふるいの方法を仮定を設けた上で適用することにより、ｎを充分大な整数とした場合にはかかる条件を充たすｎ以下の素数の個数はｄを固定した場合にはＯ（$n^{1/2}$／log ｎ）であろうとハーディ（Hardy）等により１９２３年頃から推測されている。ただし、証明はなされていない。）

③類多項式$H_d$（ｘ）のｐを法とした解を求めるステップ

ｄ＝１９のとき、

$H_{19}(x) = x + 884736$

となるのでｐを法とした解は、

$x \equiv -884736 \pmod{p}$

である。

【００７７】④楕円曲線Ｅの決定ステップ

$H_d$（ｘ）のｐを法とした解をｊ不変数にもつ有限体ＧＦ（ｐ）を定義体にもつ楕円曲線Ｅは、ＧＦ（ｐ）同型を同一視すると次の二つである。

$E_1: y^2 = x^3 + 185691005893171199485988223 07x + 990352031430246397258603863 2$

$E_2: y^2 = x^3 + 185691005893171199485988223 07x + 136173404321658879623058029 91$

各楕円曲線$E_1$のＧＦ（ｐ）上の元で構成される群$E_1$（ＧＦ（ｐ））の元の個数＃$E_1$（ＧＦ（ｐ））はいずれかがｐになり、他方がｐ＋２になる。（ｉ＝１、２）$E_1$であるか$E_2$であるか決定するにはとそれぞれの群から零元と異なる一点をとってその位数を求め、位数がｐになる方が求めるｐ個の元をもつ楕円曲線になる。実際には元をｐ倍した結果が零元になればその元の位数をｐとなることから、$E_1$（ＧＦ（ｐ））上の零元と異なる任意の元をベースポイントとする離散対数問題には、＃$E_1$（ＧＦ（ｐ））とｐが互いに素でないので帰着法を適用することができない。

【００７８】このため、有限体上の離散対数問題に帰着するという解法は存在しない。よって公開鍵暗号をかかる$E_1$（ＧＦ（ｐ））上の離散対数問題の困難性に基づくように構成すれば、秘密送信を高速になしえ、また十分な安全性が確保される。また従来の方法により、公開鍵暗号の安全性の根拠である離散対数問題を定義する有限可換群として適当な楕円曲線の構成を行うと、ＧＦ（２）上の楕円曲線を拡大体ＧＦ（$2^n$）に持ち上げるという方法で構成するため、ｎビットの大きさの有限体上の提供できる楕円曲線の個数が限られる。

【００７９】本発明は、任意の素数ｐに対して楕円曲線を構成すると、ｎビットの定義体上の提供できる楕円曲線は、少なくともｎビットの素数の数以上存在するので、$2^n$／ｎ以上のオーダ存在することになる。また従来の方法により、公開鍵暗号の安全性の根拠である離散対数問題を定義する有限可換群として適当な楕円曲線の構成を行うと、ＧＦ（２）上の楕円曲線を拡大体ＧＦ（$2^n$）に持ち上げるという方法で構成するため、非常に大きい数の素因数分解を要求し、場合に依っては非常に時間がかかる。

【００８０】本発明は、実施例の有限体ＧＦ（ｐ）上の楕円曲線$E_1$が与えられると、＃$E_1$（ＧＦ（ｐ））＝ｐとなるので素因数分解をする必要がない。なお、上述の実施例は正整数ｄを１９として行ったが、これは勿論他の虚二次体Ｑ（（－ｄ）$^{1/2}$）の類数が小さくなるような正整数であってもよい。また、ｄに対して条件を満たす素数ｐは上述の実施例だけではないので、他の素数に対しても同様にできる。

【００８１】これを以下に例示する。ｄ＝１１の場合

（２）素数ｐの生成ステップ

p=100000000000069784500614201619

$4p-1=11*190692517849185^2$

（３）類多項式Ｈｄ（ｘ）のｐを法とした解

$H11(x) = x + (2^5)^3$

$x = -(2^5)^3$

（４）

$E1: y^2 = x^3 + 646582192025387235466738614 91x + 617190295194809357160578526 4$

G1＝(0, 6865183583979787478040658432 8)

Et

$E2: y^2 = x^3 + 442350729387578836099258670 87x + 805264725178723614921944554 88$

G2=(16697588126171207059471759083, 50558135212291882814045164247)

このとき、Ｅ１が求めるｐ個の元をもつ楕円曲線

ｄ＝４３の場合

（２）素数ｐの生成ステップ

p=100000000000067553784390207169

$4p-1=43*96448564434115^2$

（３）類多項式Ｈｄのｐを法とした解

$H43(x) = x + (2^6 * 3 * 5)^3$

$x = -(2^6 * 3 * 5)^3$

（４）

E1: $y^2=x^3+24557754467536921757954818421x+40410589573449782367660219353$

G1=(26585494950223134888454565943, 31209183043559574170523404221)

E2: $y^2=x^3+69866461751524010602318419904x+17027175709313123626175488922$

G2=(0, 22374848214481414259811678518)

このとき、Ｅ１が求めるｐ個の元をもつ楕円曲線

ｄ＝６７の場合

（２）素数ｐの生成ステップ

p=100000000000039914906156290257

$4p-1=67*77266740928641^2$

（３）類多項式Ｈｄのｐを法とした解

$H67(x)=x+(2^5*3*5*11)^3$

$x=-(2^5*3*5*11)^3$

（４）

E1: $y^2=x^3+98022179152870100941803577754x+86872543342359746381224718825$

G1=(87207836128793306663103094884, 62397242280665662684542866784)

E2: $y^2=x^3+40646160753795093333095479225x+64440828019096112476624894792$

G2=(0, 23587158762484987674589379428)

このとき、Ｅ２が求めるｐ個の元をもつ楕円曲線

ｄ＝１６３の場合

（２）素数ｐの生成ステップ

p=1000000000000088850197895528571

$4p-1=163*49537740461829^2$

（３）類多項式Ｈｄのｐを法とした解

$H163(x)=x+(2^6*3*5*23*29)^3$

$x=-(2^6*3*5*23*29)^3$

（４）

E1: $y^2=x^3+69539837553085885644029440781x+21802102936259342347911085254$

G1=(0, 12971938705191708351900354586)

E2: $y^2=x^3+43531628057513197797823922759x+63587736557778697031371252331$

G2=(27229586870506933835795892372, 7702158417267369660619109104)

このとき、Ｅ２が求めるｐ個の元をもつ楕円曲線

実施例２

図７は上記実施例１で求めた楕円曲線を用いた公開鍵暗号通信方式を楕円曲線上のエルガマル暗号として具体的に実現する本発明の実施例２における方法を示すものである。そして、この基本は〔発明の背景〕で説明したのと同じである。なおまた、一般の楕円曲線上のエルガマル暗号については記述の“A course innumber theory and cryptography”に詳しく述べられている。（楕円曲線によるエルガマル暗号を使用した秘密通信）

①初期設定

上記実施例１により求められた有限体ＧＦ（ｐ）上定義された楕円曲線$E_1$ と$E_1$ （ＧＦ（ｐ））の元$G_1$ をとる。このとき$E_1$ と$G_1$ がこの暗号方式の公開情報である。

【００８２】②鍵生成

このシステムの任意ユーザＢは、任意の整数$x_B$ を選び、$E_1$ （ＧＦ（ｐ））上で

$$Y_B = x_B G_1 \quad \cdots〔1〕$$

を計算する。そこで、ユーザＢは$x_B$ を秘密鍵として保持し、$Y_B$ を公開鍵として全ユーザに知らせる。

【００８３】③暗号化

ＡからＢへ$E_1$ （ＧＦ（ｐ））の元である平文Ｍを秘密通信する場合を考える。Ａは秘密に整数である乱数ｋを選び、自分だけが知っているこの乱数ｋとＢの公開鍵$Y_B$ を用いて次の２組の暗号文$C_1$ 、$C_2$ を作成する。

【００８４】

$$C_1 = kG_1 \quad \cdots〔2〕$$

$$C_2 = M + kY_B \quad \cdots〔3〕$$

ＡはＢに$C_1$ 、$C_2$ を送る。図８に、この〔３〕式の演算をなす回路を示す。本図において、１は２進数の桁上げ加算をなす加算器である。また通信文Ｍと鍵ｋ$Y_B$ とは２進数化されている。

【００８５】④復号

Ｂは自分だけが知っている$x_B$ を用いて次式を計算してＭを得る。

$$M + x_B C_1 = C_2 \quad \cdots〔4〕$$

式〔１〕、〔２〕、〔３〕、〔４〕のいずれの演算も$E_1$ （ＧＦ（ｐ））上行われ、平文Ｍ、$Y_B$ 、$P_1$ は楕円曲線$E_1$ （ＧＦ（ｐ））上の元とする。

【００８６】この公開鍵暗号通信方式の安全性は、本発明の実施例１で構成した楕円曲線$E_1$ の$E_1$ （ＧＦ（ｐ））の元$G_1$ をベースポイントとする離散対数問題の困難さに依存している。この$E_1$ （ＧＦ（ｐ））上の$G_1$ をベースポイントとする離散対数問題は、＃$E_1$ （ＧＦ（ｐ））とｐが互いに素でないので帰着法を適用することができない。このため、有限体上の離散対数問題に帰着するという解法は存在しない。よって本発明の実施例２における公開鍵暗号通信方式は高速に実現で

きまた十分な安全性が確保される。

【００８７】なお、この場合の本来送信すべき情報を数値化した一次元情報たる数値と同じく一次元情報たる乱数と二次元情報たる楕円曲線の元Ｒとの演算はＲ（$r_x$、$r_y$）の$r_x$ を使用しており、別途$r_x$ からＲ（$r_x$、$r_y$）を復号可能な情報をも送信するものとしている。このような情報としては例えば、$r_y$ ＝±（$r_x{}^3$ ＋ａ＊$r_x$ ＋ｂ）$^{S+1}$（フェルマーの定理）という性質を利用して、この式の符号が－のときにはｃｕ（Ｒ）＝１、＋のときにはｃｕ（Ｒ）＝０と取り極めた上でのｃｕ（Ｒ）がある。

第３実施例

本実施例は前記第２実施例を有料の秘密放送に応用したものである。この場合、前記第２実施例における$x_B$ は、あらかじめ料金を納付した視聴者に配付した小型の復号装置に差し込まれるキーに回路的に組み込まれている。この上で、有料放送者は$C_1$ と$C_2$ を放送する。この放送波を受信した料金納付済の視聴者に配付された小型の復号装置は、Ｍ＋$x_B$ $C_1$ ＝$C_2$ という演算を行うことにより、容易にＭを得た上で、これをテレビジョン受信機本体に流す。

【００８８】更にこの場合、有料放送の契約期間は１年とし、１年毎に秘密放送の提供者は$x_B$ を変更し、すなわち$Y_B$ を変更する。そして、新しい年度に入れば、当該年度の放送料を納付した者にはこの新しいキーを配付しておく一方、この新しい$Y_B$ を使用して秘密放送をする。この際、視聴者は新しい放送年度に入れば、小型の復号装置の旧年度のキーを抜き取り、新年度のキーを差し込むことにより、秘密鍵、共有鍵の切り換えもスムーズになされる。

第４実施例

本実施例は、前記第２実施例を国際線に就航する旅客機の映像情報源の有料の貸し出しに使用したものである。この場合、前記第２実施例における$x_B$ は、あらかじめ各座席に固定装備して設けてあるマイクロコンピュータとＶＴＲつきの小型のテレビジョン映像機の本体の密閉部に設けられたキー孔に差し込まれるキーに回路的に組み込まれている。

【００８９】このため、旅客は、この小型テレビジョン映像機そのものを持ち出すか本体をこわさない限りこのキーを持ち出すことは不可能である。この上で、各旅客に貸し出す映像情報源には、$C_1$ と$C_2$ が記録されている。この映像情報源を有料で貸与された旅客は自己のＶＴＲにこの映像情報源を装備する。これによりテレビ映像機つきのマイクロコンピュータがＭ＋$x_B$ $C_1$ ＝$C_2$ という演算を行い、Ｍを得た上で小型のテレビジョン映像機に映像情報を映し出す。

【００９０】以上、本発明を実施例に基づき説明してきたが、本発明は何も上記実施例に限定されないのは勿論である。すなわち例えば、第１実施例において、４Ｐ－１＝ｄ＊平方数　となる素数は事実上無数に存在するため、楕円曲線は他のものでもよい。第２実施例において、従来技術に係るエルガマル暗号類似の手法を使用してもよい。すなわち、二人のユーザＡ、Ｂは各々$x_A$、$x_B$ を選定し、相互に$Y_A$ ＝$x_B$ $G_1$ と$Y_B$ ＝$x_B$ $G_1$ を選定の上$Y_{AB}$＝$x_B$ $Y_A$ ＝$x_A$ $Y_B$ を共有鍵として通信に使用してもよい。

【００９１】また、通信文書の暗号化、復号は回路（ハード）的になすのでなく、大型計算機を使用して計算（ソフト）で為してもよい。用途も第３、第４実施例に限定されず、署名、認証通信であってもよい。

【００９２】

【発明の効果】以上説明したように、請求項１及び請求項２の発明においては、直接的には、

①楕円曲線上の離散対数問題の解法に帰着法が適用できない。

②同じビット数の定義体上の楕円曲線を豊富に提供できる。

請求項３の発明においては、直接的には、上記①及び②を充たす楕円曲線を容易に作成可能である。

【００９３】という効果がある。ひいては、公開通信網を使用するため第三者の盗聴、詐称等を完全に防止することが困難な通信においても、その秘密性の確保、認署の確実性が図れる。また、有料の秘密放送においても無断利用の防止が図られ、情報媒体の有料貸与においても不返却の防止が図られる。

【図面の簡単な説明】

【図１】従来技術に係る送信情報の共有鍵による秘密送信の原理を示す。

【図２】従来技術に係る送信情報の共有鍵による秘密化の原理を示す。なお、下添え字の２はこれが添えられている数が２進数であることを示す。

【図３】楕円曲線上の群の加法を示す。

【図４】第１の従来例における楕円曲線の構成法を示す。

【図５】第２の従来例における楕円曲線の構成法を示す。

【図６】本発明の実施例１における楕円曲線を用いた公開鍵暗号通信方式の構成法を示す。

【図７】本発明の実施例２における楕円曲線を用いた公開鍵暗号通信方式の構成法を示す。

【図８】上記第２実施例における演算回路の構成図である。

【符号の説明】

１　　２進数用の桁上げ加算器

【図1】

| | | |
|---|---|---|
| 初期設定 | 公開鍵 | 素数 p(11)<br>原始根 q(2) |

⇓

| | | |
|---|---|---|
| 秘密鍵生成 | ユーザA | ユーザB |
| 選定 | a(4) | b(8) |
| 剰余計算 | $g^a \equiv \alpha (\mathrm{mod}\ p)$<br>(5) | $g^h \equiv \beta (\mathrm{mod}\ p)$<br>(3) |
| 交換 | $\beta$ | $\alpha$ |

⇓

| | | |
|---|---|---|
| 共有鍵作成 | $k \equiv \beta^a (\mathrm{mod}\ p)$<br>(5) | $k \equiv \alpha^b (\mathrm{mod}\ p)$<br>(4) |

⇓

秘密通信，署名通信

【図2】

情報　h ＝ $101_2$

共有鍵　k ＝ $100_2$

①

$$\begin{array}{r} 101_2 \\ \times\ 100_2 \\ \hline 10100_2 \end{array}$$

②

$$\begin{array}{r} 101_2 \\ +\ 100_2 \\ \hline 1001_2 \end{array}$$

③

$$\begin{array}{r} 101 \\ f\ 100 \\ \hline 001 \end{array}$$

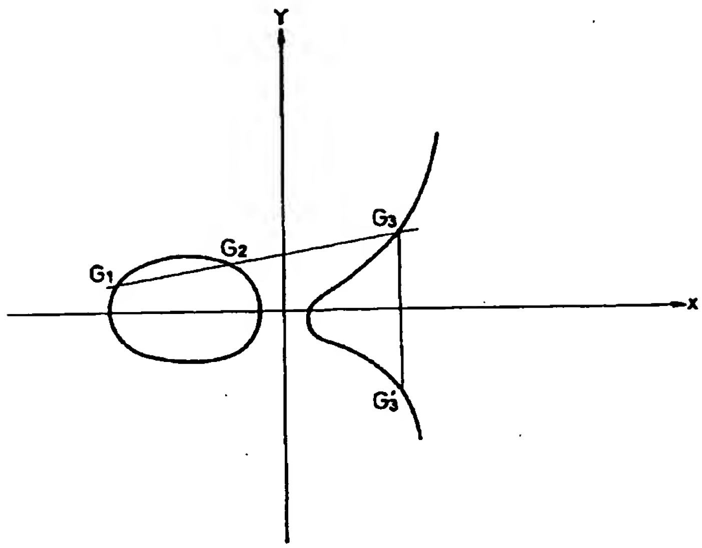
【図4】

1 楕円曲線の候補の決定

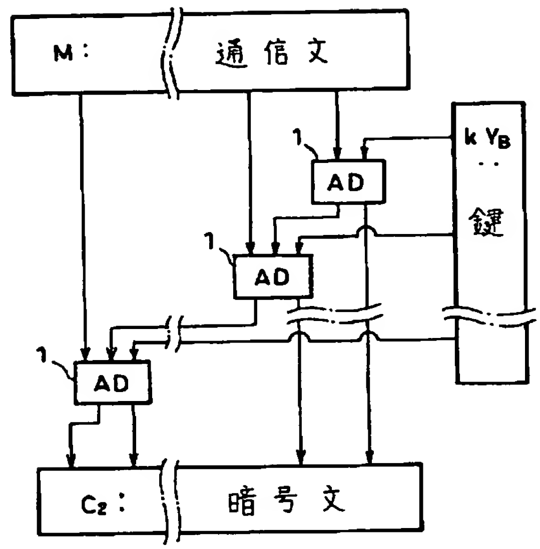
↓

2 適当な拡大次数 m の決定

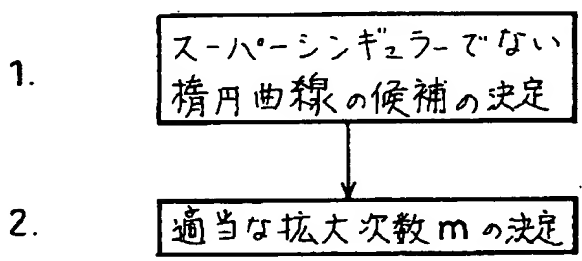
【図3】


Y
x
$G_1$
$G_2$
$G_3$
$G_3'$

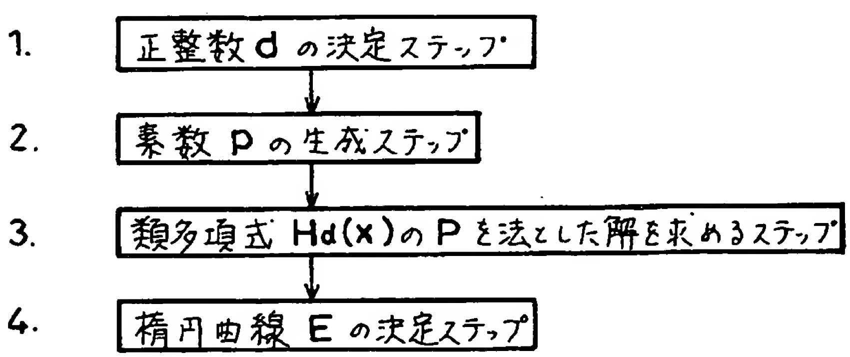
【図8】


M： 通信文
k $Y_B$ ： 鍵
1
AD
1
AD
1
AD
$C_2$： 暗号文

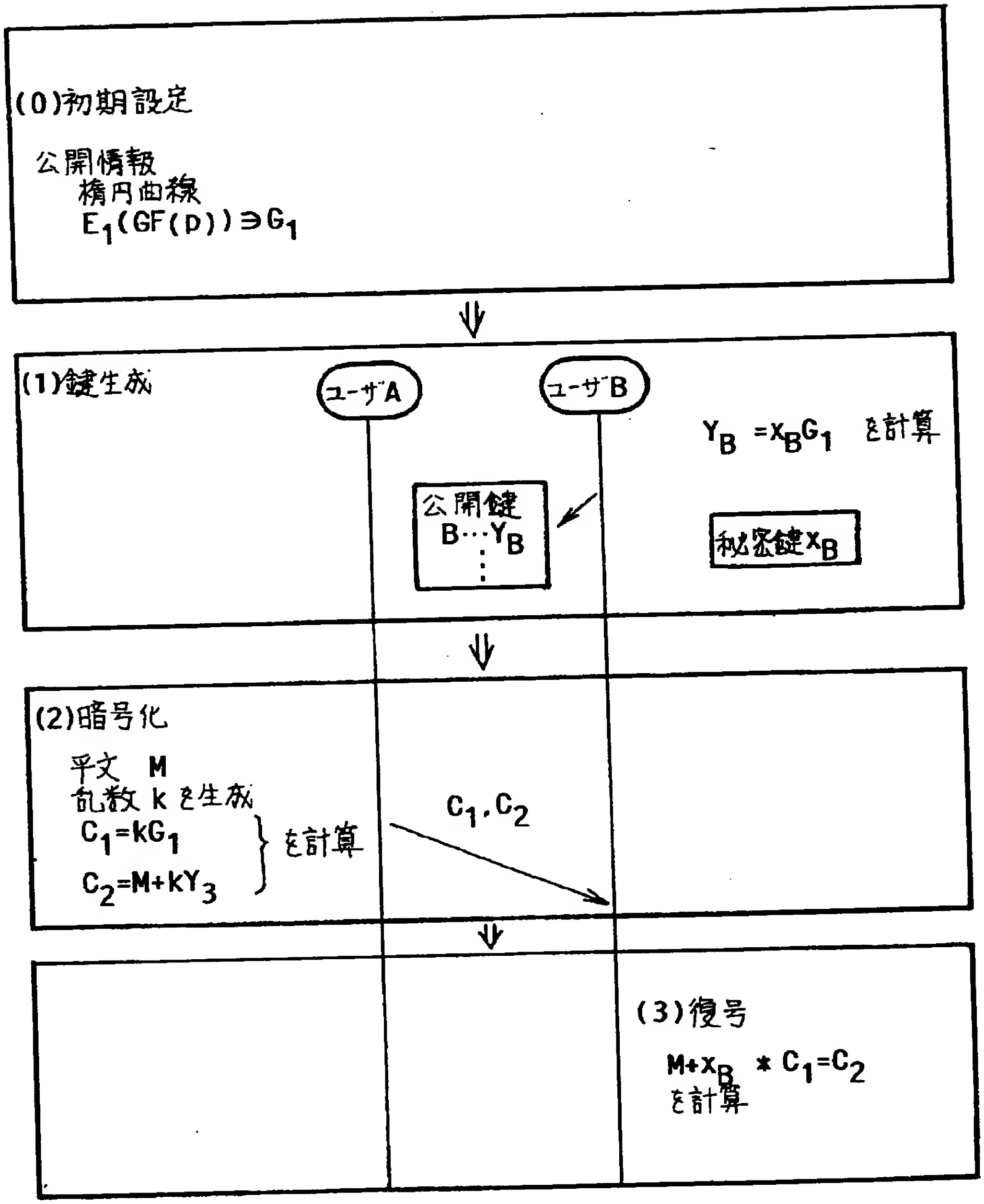
【図5】


1.
スーパーシンギュラーでない楕円曲線の候補の決定
2.
適当な拡大次数 m の決定

【図6】


1.
正整数 d の決定ステップ
2.
素数 p の生成ステップ
3.
類多項式 Hd(x) の P を法とした解を求めるステップ
4.
楕円曲線 E の決定ステップ

【図７】


(0)初期設定
公開情報
楕円曲線
$E_1(GF(p)) \ni G_1$
(1)鍵生成
ユーザA
ユーザB
$Y_B = x_B G_1$ を計算
公開鍵
$B \cdots Y_B$
秘密鍵 $x_B$
(2)暗号化
平文 M
乱数 k を生成
$C_1 = kG_1$
$C_2 = M + kY_3$
を計算
$C_1, C_2$
(3)復号
$M + x_B * C_1 = C_2$
を計算